システム監査基準（案）

経済産業省

令和５年Ｘ月Ｘ日

目次

前文（システム監査基準の活用に当たって）

・システム監査基準の意義と適用上の留意事項

システム監査とは、監査人が、一定の基準に基づいてITシステムの利活用に係る検証・評価を行い、ガバナンスやマネジメント等について、一定の保証や改善のための助言を行うものであり、システムの信頼性等を確保し、企業等に対する信用を高める重要な取組である。

今日社会でのITや情報システム、さらにはデータ・情報（本監査基準において、IT、情報システム、データ・情報をまとめた概念として「ITシステム」という。）の利活用は、会社やその他組織体の諸活動全般に及んでいる。IT システムの戦略的利活用は、組織体の価値の向上や会社の競争力の維持、向上を図る上で不可欠である一方、それに伴いリスクも増大している。組織体が適切にリスク・マネジメントを行い、価値向上のためにITシステムの利活用を適切に行うことを確実にするために、システム監査が効果的・効率的に行われることが必要である。

システム監査が効果的かつ効率的に行われるためには、システム監査のあるべき体制や実施方法等が示される必要がある。この「システム監査基準」(以下、「本監査基準」という。）は、このニーズに応えるために制定されている。

なお、近年デジタル・トランスフォーメーション（以下、「DX」という。）を進める上でも鍵となるデジタル技術等を含める概念として、「テクノロジー」という用語も用いられているが、本監査基準では、ITという用語をその意味も込めて用いている。

本監査基準は、システム監査実施の前提となる「システム監査の意義と目的」、「監査人の倫理」と監査の体制や実施のあり方を示した「システム監査の基準」から構成されており、組織体の監査役（会）等（監査役設置会社の監査役会及び監査役、等）や内部監査部門等が実施するシステム監査だけでなく、組織体の外部の第三者に依頼するシステム監査においても適用される。また、取締役や経営者、管理者がガバナンスやマネジメントの視点から IT システムの利活用を監視、監督、あるいは点検や確認等を行う際にも参考になるものである。

さらに、本監査基準は、中小規模の企業や、各府省庁、地方公共団体、病院、

学校法人等、各種組織体が各種目的をもってシステム監査を行う場合にも利用ないし参考にできるように、汎用性のある内容となっている。

・システム監査上の判断尺度

本監査基準に基づくシステム監査においては、IT システムのガバナンス、マネジメント、コントロールを検証・評価する際の判断の尺度として、「システム管理基準」又は当該基準を組織体の特性や状況等に応じて編集した基準・規程等を利用することが望ましい。なお、システム監査は各種目的あるいは各種形態をもって実施されることから、他のガイドラインや組織体独自の諸規程・マニュアル等を、システム監査上の判断尺度として用いることもできる。特に、情報セキュリティの監査に際しては、「システム管理基準」とともに、「情報セキュリティ管理基準」も参照することが望ましい。

・本監査基準改訂の背景と主要な改訂内容

本監査基準は、昭和 60 年（1985 年）１月に策定され、その後、平成８年(1996 年)１月、平成 16 年（2004 年）10 月、平成 30 年４月（2018 年）に改訂がされてきたが、その後もシステム監査を巡る IT 環境の継続的な変化や、システム監査に対するニーズの多様化がみられたことから、それらを踏まえて基準の構成や内容を見直しすることとした。

具体的な環境変化やニーズの多様化とは、AI の発展と DX の普及、システム・マネジメントの基となるガバナンスの重要性増加、いわゆるスリー・ラインズ・モデル等で言われる各種のモニタリング活動とシステム監査の連携の重要性増加、アジャイル監査の普及等監査方法の多様化等である。更に言えば、組織体の目的・目標の達成のために、カメラやセンサー、聴音機等からの情報が産業システムに送られ、さらにそのデータが情報システムである AI に送られ、AI がそのデータを分析するといった産業システムと情報システムの連携・協働といったテクノロジーの利活用も行われてきている。

当然のことながら、システム監査の基本的な原則や規準は普遍的なものであり頻繁に変えられるべきものでないものの、こういったシステム監査を取り巻く技術革新や社会情勢の変化等の環境の変化に対応してこそ、本監査基準はよ

り有効なものとなる。

そのため、今回の改訂においては、システム監査に係る文書として、監査にとって普遍的な内容は本監査基準に記述し、実施方法等のシステム監査を取り巻く環境の変化への対応が期待されるより具体的な内容については、環境の変化へのより迅速な対応が可能となるよう、システム監査基準ガイドライン（以下、単に「ガイドライン」という。）を新たに民間団体により整備するという体制に変更することとした。

また、今回の改訂では、「システム監査の基準」の前に「システム監査の意義と目的」と「監査人の倫理」の項目を設けている。

「前文」に続き、最初に「システム監査の意義と目的」の項目を設けた意図は、監査人に求められる倫理及びシステム監査に要求される具体的な基準の内容は、「システム監査の意義と目的」に基づいて決まっていくことからである。逆にいえば、「システム監査の意義と目的」を達成するための倫理と基準である必要がある。

次に「監査人の倫理」の項目は、倫理が適切な監査行為の前提となるため、「システム監査の基準」の前に置いた。監査人が、システム監査に期待されている様々なシステム監査の意義と目的を達成するためには、監査人は高い倫理が要求される。監査という外面的な行為を導く内面の倫理が監査の品質を担保する根本的な要素となる。前述のように IT やシステム監査を巡る環境変化が著しい昨今、本監査基準やガイドラインを適切に運用していく上でも倫理は必須となる。倫理を土台に監査人が監査の目的を達成する監査を実施していくことで、監査人は信頼を得ることになる。

なお、本監査基準では、「監査人の倫理」は監査人の立場から、「システム監査の基準」はシステム監査機能の立場から記述している。倫理は最終的には個々の監査人に帰せられるべき事項であるのに対して、監査はシステム監査機能（監査人や監査チーム等の提供する機能）のあり方を示す必要があるからである。

また、各基準の補足的な説明や、実務上の望ましい対応や留意事項を「解釈指針」として記述した。

・監査人と取締役会等、経営者との関係

本監査基準において、監査人とは、独立にして客観的な立場から情報システムに係る保証や助言の活動を行う者を指し、ガバナンスの一翼を担う会社法上の監査役（会）等とその補助使用人、内部監査人、組織体からの依頼により監査を行う組織体の外部の第三者が含まれる。

監査役（会）等は、法令の定めるところにより株主からの委任により、取締役の業務執行に対する監査の一環としてシステムに係る監査を行う。したがって、ガバナンスに対する監査を実施することになる。

内部監査人や外部監査人は、取締役会等（取締役会、理事会等）や経営者からの委託により、IT システムに係る監査を実施し、その結果を報告することによりガバナンス､マネジメント､コントロールに役立つ監査を行うことになる。なお、取締役会等からの指示や監査役（会）等からの依頼により内部監査人や外部監査人がガバナンスに対する監査を行うこともあり得る。

また、監査業務は保証を目的としたシステム監査と助言を目的としたシステム監査から成り立っている。

保証を目的としたシステム監査には、組織体、業務、機能、プロセス、情報システム又はその他の対象事項（以下、「監査対象先」という。）について、監査の意見又は結論を得る基礎として、監査人が入手した証拠を客観的に評価することが含まれる。保証を目的としたシステム監査の内容と範囲は、監査人が決定する。一般的には、

次の三者が当事者となる。

(1)　プロセス・オーナー：事業体、業務、機能、プロセス、システム若しくはその他の監査対象事項に直接関わる者又はグループ、

(2)　監査人：評価を行う者又はグループ

(3)　利用者：評価結果を利用する者又はグループ

システム監査においては、プロセス・オーナーには監査対象先が、監査人には内部監査人や外部監査人が、利用者には経営者や取締役会等が一般的には該当する。なお、外部監査の場合には、組織体外部の第三者にシステム監査の実施を依頼する者がおり、取締役会、経営者等がその監査の依頼者となる。

また、監査役（会）等の監査においては、プロセス・オーナーには取締役や監査対象先が、監査人には監査役（会）等が、利用者には株主が一般的には該

当する。

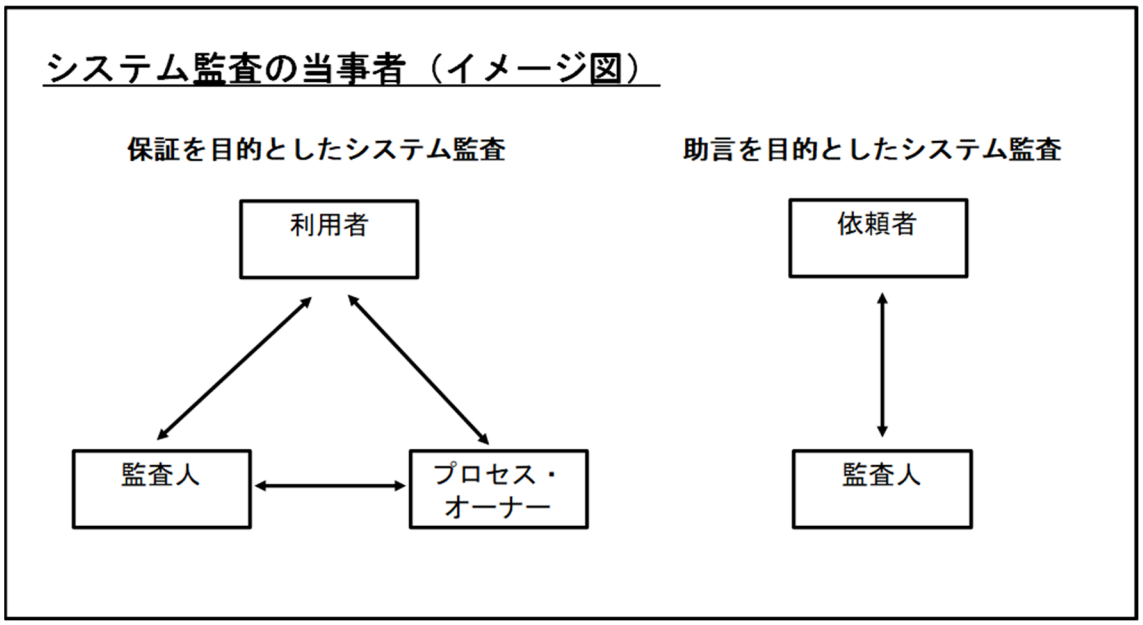
助言を目的としたシステム監査の性質は、助言に加えて提案や相談の提供であり、一般に、依頼者からの具体的な要請に基づいて実施される。個々の助言業務の内容と範囲は、依頼者との合意による。一般的には、助言を目的としたシステム監査では、次の二者が当事者となる。

(1)　監査人：助言を提供する者又はグループ

(2)　依頼者：助言を必要として、これを受ける者又はグループ

ただし、監査の性格においては、当事者が増加ないし変化する場合がある。

助言業務を実施するに当たっても、監査人は、客観性を維持すべきであり、また、管理者としての職責を負ってはならない。



・本監査基準への適合

本監査基準の記述形式については、システム監査の実施に際して適合が求められる「基準」を「しなければならない」と記述し、各基準の補足的な説明や、実務上の望ましい対応や留意事項を「解釈指針」として記述した。

本監査基準に沿って監査を実施した監査人は、必要な場合には、実施したシステム監査を本監査基準に適合して実施したことを説明しなければならない。

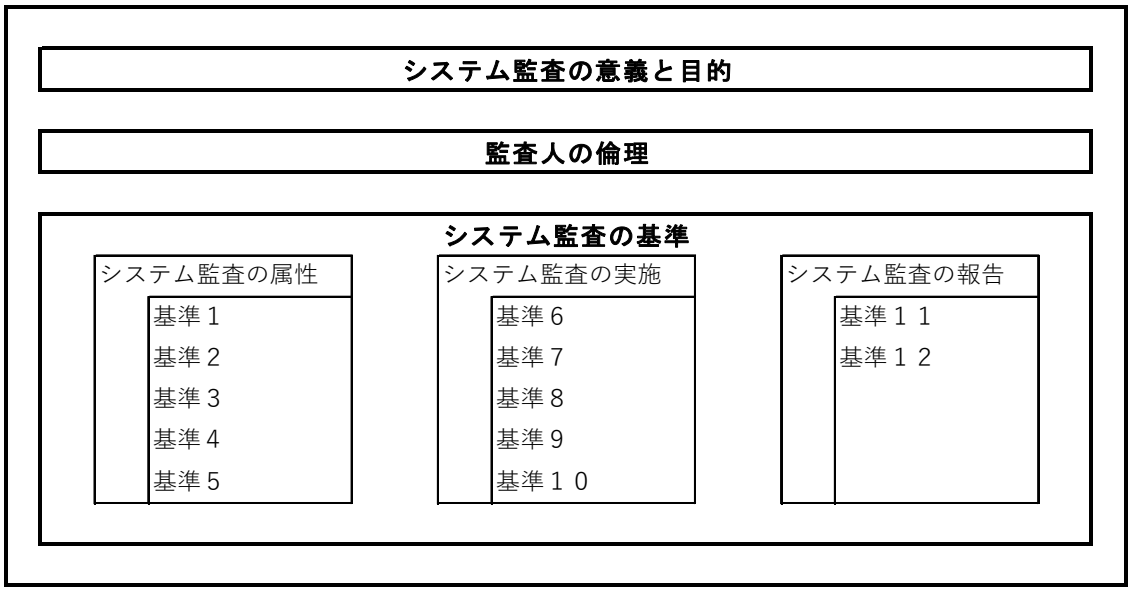
また、法令の定めや環境等により、本基準の特定部分への適合が制約されることがある場合や適合できなかった部分がある場合は、その制約の内容や適合

できなかった部分を、その理由とともに開示する必要がある。

なお、本監査基準を他の権威ある機関から出されている要求事項（以下、「他の要求事項」という。）とともに用いるときには、必要な場合は使用した他の要求事項についても言及しなければならない。

また、本基準で用いられる用語とその用法については、用語集に説明が記載なされており、この用法に従って本監査基準は読まれる必要がある。

【参考】システム監査基準の概観



システム監査の意義と目的

システム監査とは、専門性と客観性を備えた監査人が、一定の基準に基づいてITシステムの利活用に係る検証・評価を行い、監査結果の利用者にこれらのガバナンス、マネジメント、コントロールの適切性等に対する保証を与える、又は改善のための助言を行う監査である。

また、システム監査の目的は、ITシステムに係るリスクに適切に対応しているかどうかについて、監査人が検証・評価し、もって保証や助言を行うことを通じて、組織体の経営活動と業務活動の効果的かつ効率的な遂行、さらにはそれらの変革を支援し、組織体の目標達成に寄与すること、及び利害関係者に対する説明責任を果たすことである。

監査人の倫理

システム監査は、監査人の誠実性及び専門的な能力を信頼し依頼されるものであり、監査人はその期待に応え、責任を果たすことが求められ、業務に関する説明責任を果たすこととなる。

さらに、システム監査が結果として、広く社会的な信用につながるには、個々の依頼人の要請を満たすだけではなく、監査人が独立した立場において、社会的役割を自覚し、自らを律し、かつ社会の期待に応え、公共の利益に資することができなければならない。

IT の進展をはじめ、監査の対象となるシステムを巡る環境変化が激しいこともあり、監査の方法の選択や監査結果の判断に関して、種々の価値観の中で適切な意思決定をするためには、監査人の倫理が重要である。加えて、IT 利活用の高度化により、システム監査においても機密性の高い情報に触れる機会が増加しており、倫理に関して社会的な要請が高まっていることを意識しなければならない。

倫理に関して監査人が守るべき４つの原則を以下に明示する。

○ **誠実性**

監査業務において、常に正直な態度を保持し、強い意志をもって適切に行動すること。監査人が誠実であることによって信頼が築かれることから、誠実性は、自らの判断が信用される基礎となる。

○ **客観性**

監査業務において、バイアス（先入観等）、利益相反を排し、個人や組織等から不当な影響を受けることなく、監査人としての判断を行うこと。監査人としての判断が不当な影響を受ける場合、当該業務を引き受けてはならない。

○ **監査人としての能力及び正当な注意**

監査業務において、必要な知識、技能を習得し、維持すること、及び誤った監査上の判断がないように、システム監査の基準に従って、監査人として当然払うべき注意を払うこと。

○ **秘密の保持**

監査業務において、取得した情報の秘密性を尊重し、業務上知り得た秘密を守ること。法令等による守秘義務の解除を除き、依頼人又は所属する組織との関係が終了した後も、秘密の保持が求められる。

システム監査の基準

［１］システム監査の属性に係る基準

【基準１】システム監査に係る権限と責任等の明確化

システム監査を実施する意義、目的、対象範囲、並びに監査人及びシステム監査を行う組織の権限と責任は、文書化された規程等により定められていなければならない。

＜主　　旨＞

効果的かつ効率的なシステム監査を実現するための体制整備として、監査人及びシステム監査を行う組織の権限と責任を組織体の内部監査規程等によって明確にし、組織体全体に周知しておく必要がある。

また、システム監査を外部委託する場合には、委託先の権限と責任を契約書等の文書で明確に定めておく必要がある。

＜解釈指針＞

1. システム監査を行う組織は、効果的かつ効率的なシステム監査を実現するため、システム監査に関する規程を整備する。システム監査に関する規程は、組織体の内部監査規程の一部として、あるいは内部監査規程とは別に定められる。

   システム監査に関する規程は、内部監査規程と同様の承認プロセスを経た上で、組織体全体に周知される。

2. 組織体の内部にシステム監査を行うのに適切な監査人が存在しない場合、システム監査の実施に高度な技能を必要とする場合、遠隔地の監査対象先にシステム監査を実施する場合等においては、システム監査の全部又は一部を、組織体外部の専門家（監査法人等を含む）に委託する場合がある。

   このような場合には、委託契約書等の文書に、委託するシステム監査業務の内容、及び受託する専門家の権限と責任等を明確に記載する。

   (1) システム監査の全部又は一部を組織体外部の専門家に委託する場合、当該専門家と密接に連携し、当該専門家に対する適切な監督を行うことが重要である。

(2)　外部委託先の専門家は、原則として、委託元の組織体と身分上又は経済上の特別な利害関係を有してはならない。密接な利害関係を有する者を外部委託先とする場合は、システム監査業務に影響を及ぼさぬよう適切な措置を講じなければならない。

(3)　システム監査の全部又は一部を組織体外部の専門家に委託する場合であっても、組織体のシステム監査を行う組織の長は、システム監査の最終的な責任は自らにあることを認識しなければならない。

【基準２】専門的能力の保持と向上

適切な教育・研修と実務経験を通じて、システム監査に必要な知識、技能及びその他の能力を保持し、その向上に努めなければならない。 **また、組織体のシステム監査を行う組織の長は、効果的かつ効率的なシステム監査に必要な知識、技能及びその他の能力を、システム監査を行う組織が総体として備えているか、又は備えるようにしなければならない。**

＜主　　旨＞

システム監査の信頼性を保つためには、専門的な観点からシステム監査が実施される必要がある。また、組織体の状況変化や IT 環境の変化に対応した品質の高いシステム監査を実施するためには、IT システム及びシステム監査に関する専門的知識や技能を保持する必要があり、さらに論理的思考能力やコミュニケーション能力等も求められる。

継続的な教育・研修と実務経験を通じて、効果的かつ効率的なシステム監査を行えるよう、必要な知識、技能及びその他の能力の向上を図ることが必要である。

＜解釈指針＞

1.　システム監査を効果的かつ効率的に実施するためには、システム監査の目的や対象範囲に応じて、適切な知識や技能を有する者がシステム監査を実施する必要がある。

(1)　例えば、サイバー攻撃等の対策が効果的に実施されているかどうかの監査が求められる場合と、IT システムのガバナンスが適切に機能しているかどうかの監査が求められる場合とでは、監査人に求められる知識や技能は異なったものとなることが想定される。システム監査それぞれの目的や対象範囲に応じて、適切な知識や技能を有する者がシステム監査を担当する必要がある。

(2)　システム監査の実施に必要な知識や技能の保持及び向上には、組織体内外の講習会等の活用と併せ、OJT 等を通じた実務経験も重要である。

2.　IT システムのガバナンスとマネジメント、及びシステム監査に関する基

本的な知識や技能に加えて、経営戦略、ガバナンス、リスク・マネジメント、内部統制及び関連法令等に関する幅広い関連知識を有することが求められる。なお、システム監査の目的や対象範囲によって必要な知識や技能は異なるため、一人一人の監査人に全ての知識と技能が要求される訳ではなく、システム監査を行う組織が総体として知識や技能を備えることが求められる。

3. システム監査を取り巻く環境変化を常にキャッチアップし、新しい知識や技能を習得し続ける努力が求められる。特に、情報システムリスクの変化に対する認識を高めることは重要である。

【基準３】システム監査に対するニーズの把握と品質の確保

システム監査の実施に際し、システム監査に対するニーズを十分に把握した上でシステム監査業務を行い、システム監査の品質が確保されるための体制を整備・運用しなければならない。

＜主　　旨＞

システム監査は、任意監査（法令等で義務付けられていない監査）であることから、基本的にはシステム監査の利用者（保証業務の場合）又は依頼者（助言業務の場合）のシステム監査に対するニーズを十分に踏まえたものでなければならない。

また、システム監査に対するニーズを満たしているかどうかを含め、一定の監査品質を確保するための体制を整備・運用することが必要である。

＜解釈指針＞

1.　システム監査を実施する場合、システム監査の利用者又は依頼者のニーズに見合ったシステム監査の目的が決定され、システム監査の対象が選択される。

(1)　システム監査の目的は、以下のようなニーズに基づいて決定される。

①　経営者が、取引先等からの信頼を得るために、経営者による言明書の範囲内で、自組織体の IT システムのマネジメントが有効に機能していることのお墨付きを得たいというニーズをもっている場合、「システム管理基準」に照らして IT システムのマネジメントの状況を検証・評価し、もって保証を目的としたシステム監査が行われる。

②　経営者が、自組織体のシステム開発管理に重大な不備があるのではないかと不安に思っており、もし不備があればそれを指摘してもらい、改善の具体的な方策を知りたいというニーズをもっている場合、「システム管理基準」に照らして現状のシステム開発管理の状況を検証・評価し、指摘とともに改善提案を行う、助言を目的としたシステム監査が行われる。

なお、上記②の目的をもったシステム監査を行って成熟度が確認できた時点で、①の目的をもったシステム監査が行われることが通例である。

(2)　システム監査の対象は、以下のようなニーズに基づいて選択される。

①　経営者が、経営戦略とIT戦略との整合性、ITシステムの利活用の有効性、企業グループ全体としてみた場合のIT戦略の合理性についての保証又は助言を得たいというニーズをもっている場合、ITシステムのガバナンスを対象とするシステム監査が選択される。

②　経営者が、情報システムのサービスレベルの維持、より効率的な情報システムの維持管理、プライバシー規制等への対応状況について保証又は助言を得たいというニーズをもっている場合、情報システムのマネジメントを対象とするシステム監査が選択される。

③　経営者が、情報システムに実装された機能要件が、業務要件の変化に対応して適切に維持管理が行われているかどうかについての保証又は助言を得たいというニーズをもっている場合、情報システムのコントロールを対象とするシステム監査が選択される。

なお、上記の①、②及び③は、それぞれ別個の監査対象として明確に区別されて選択される場合もあれば、特に区別されずに組み合わせて選択される場合もある。

2.　システム監査の品質を維持し、さらにはシステム監査業務の改善を通じてその品質を高めるために、システム監査を行う組織での自己点検・評価（内部評価）、及び組織体外部の独立した専門家による点検・評価（外部評価）を定期的に実施することが望ましい。

内部監査として実施するシステム監査の場合には、一般社団法人日本内部監査協会の「内部監査基準」や内部監査人協会（IIA）の「専門職的実施の国際フレームワーク」を参照して品質を高めることにも留意する。

システム監査の品質の維持及び向上に際しては、システム監査に対するニーズに十分に応えているかどうかという視点を組み込むことが重要である。

自らの業務を継続的又は定期的に見直し、その結果をシステム監査業務

の改善に結び付ける努力こそ、システム監査の品質を保ち、向上させるための鍵となることに留意すべきである。自らの業務を本監査基準やベストプラクティス等に照らして見直し、改善のための工夫を凝らす試みは、監査人の能力向上にもつながる。

3. システム監査終了後、監査の依頼者や利用者から監査人が実施した監査内容について意見を聴取したり、監査対象先からアンケート調査等によって監査人が実施した監査の方法や結果等に関する評価を求めたりすることも、システム監査の品質の維持及び向上にとって有益である。

4. システム監査を外部の専門家に委託して実施する場合にも、委託先における監査の品質管理体制を確かめておくことが必要である。

【基準４】監査の独立性と客観性の保持

システム監査は、監査人によって誠実かつ、客観的に行われなければならない。 **さらに、監査人が監査対象の領域又は活動から、独立かつ客観的な立場で監査が実施されているという外観にも十分に配慮されなければならない。**

＜主　　旨＞

システム監査は、客観性、誠実性の保持として、客観的な立場で公正な判断を行うという精神的な態度を堅持する監査人によって行われなければならない（精神的独立性）。

監査人の精神的独立性は当然であるが、さらにシステム監査は、組織体の内部監査部門で行われるものであれ、外部の専門事業者によって行われるものであれ、監査対象先から独立した立場で実施されているという外観が確保される必要がある（外観的独立性）。

＜解釈指針＞

1. システム監査の実施に当たり、精神的独立性が堅持できない場合には、システム監査における客観性、ひいてはシステム監査の品質が維持できず、信頼性を著しく毀損することになることに留意する。
2. 監査人に精神的独立性が欠けるという疑いや印象を与えないために、システム監査は監査対象先から独立した監査人によって行われる必要がある。

   所属する部門が、監査対象の領域又は活動と同一の指揮命令系統に属する場合、組織的な独立性が毀損されているとの外観を呈することに留意する。
3. システム監査を外部の専門事業者（専門家）に委託する場合、システム監査を担当する者が、専門家としての能力を有しているか、独立性に問題がないかを確かめることが求められる。

   委託元組織体と身分上の密接な利害関係を有することは、独立性が毀損されているとの外観を呈することに留意する（システム監査を外部に委託する場合の独立性については、【基準１】解釈指針２．(2)参照のこ

と)。

【基準５】監査の能力及び正当な注意と秘密の保持

システム監査は、専門的能力の維持・向上を図るとともに、監査業務において正当な注意を払って実施する監査人によって行わなければならない。また、監査人は秘密の保持をしなければならない。

＜主　　旨＞

システム監査は、監査計画策定等の監査業務を行う際、独立性と客観性の保持と併せて、監査の専門家として要求される正当な注意を払い、秘密の保持の遵守により監査業務の品質を確保する監査人によって行われなければならない。

＜解釈指針＞

1. システム監査の実施に当たり、客観的な立場で公正な判断が行われるために、専門的な知識・技能を有する監査人によって行わなければならない。専門的な知識・技能を習得し、維持することは、監査人としての能力をもって依頼者に保証・助言を提供するために、適切な判断をすることが求められるからである。

   また、システム監査は、監査人としての正当な注意を払い、また正当な懐疑心をもって、標準的な監査人が同様な監査をした場合に見逃すことのないリスクを的確に識別することが重要である。IT システムの利活用に係る監査においては常に組織体内外の状況とその変化に目を向けて、組織体の論理や価値観だけで判断を行うのではなく、社会的な視点からみて公正な判断を行うことが望まれることを留意する必要がある。特に、IT の進展をはじめ、デジタル技術の変化によるリスク、システム開発手法の変化によるリスクに注意を払う必要がある。

2. システム監査の実施に当たり、業務上知り得た事項を正当な理由なく他に開示したり、自らの利益のために利用したりしてはならないことが監査人に求められる。なお、秘密の保持は、所属する職業団体や会社における倫理規程、契約、就業規則等によって要求される場合もある。

［２］システム監査の実施に係る基準

【基準６】監査計画の策定

システム監査を効果的かつ効率的に実施するために、適切な監査計画が策定されなければならない。 監査計画は、主としてリスク・アプローチに基づいて策定する。 監査計画は、リスク等の状況の変化に応じて適時適切に見直し、変更されなければならない。

＜主　　旨＞

1. 監査計画の必要性

監査の網羅性と効率性を整合させ、有効性の高いシステム監査の実施のためには、その目的達成に必要十分な事項を記載した適切な監査計画を策定する必要がある。

2. リスク・アプローチ

① 監査計画の適切性を確保するためには、主として監査対象のリスクの大きさや重要性等に基づいて策定される必要がある。

② 監査計画の適切性を維持するためには、監査対象の変化（リスクや重要性等の変化）に応じて、適時適切に見直し、変更されるとも必要である。

＜解釈指針＞

1. 監査計画の必要性

(1) 監査計画は、監査の網羅性を確保し、かつ監査リスクを合理的に低い水準に抑えた効果的・効率的な監査を実施するために、監査の基本方針を策定し、監査の具体的内容（例えば、目的・目標、実施時期、適用範囲、及び監査の方法等）を決定する。

(2) システム監査の対象となり得る範囲は、原則として組織体及びその集団における IT システムの利活用に係る経営活動及び業務活動の全てである。監査において実際に監査を実施しなければならない可能性のある

領域を、監査対象領域（Audit Universe）と呼ぶことがあるが、システム監査の対象となり得る範囲は、この監査対象領域の IT システムの利活用に係る領域である。

監査計画（中長期、年度、個別）策定においては、組織体及び組織体集団において IT に係る監査対象領域に基づいて具体的な監査範囲を決定する。その際に組織体にとって受容できないリスク又は重要なリスクが存在する可能性があると合理的に推測できる範囲（組織、業務プロセス等）を全てシステム監査の対象範囲に含めなければならず、その決定の合理性を説明できなければならない。

(3) 監査は、監査目的に基づき、ガバナンス、マネジメント、コントロール、及びこれらの統合的視点から検証する必要がある。

① ガバナンスの視点:IT システムに係るガバナンスを監査対象とする場合、取締役会等が IT システムの利活用について経営目的や経営戦略に沿うように経営者に対して適切な方向付けを行い、指示し、かつ、経営者の執行状況を監督し、必要な場合には是正措置を適切に指示しているかどうかを確かめることに重点を置いた監査計画となる。例えば、IT 戦略は経営戦略と整合しているか、新技術や技術革新を経営戦略推進のために適時適切に利活用できているか等を監査する計画が必要となる。また、マネジメントの視点、コントロールの視点での監査により識別した重大な不備やリスクの根本的発生原因がガバナンスにあると推察される場合は、その点についても検証する必要がある。

② マネジメントの視点:IT システムの利活用に係るマネジメントを監査対象とする場合、経営者による方向付けに基づいて、PDCA サイクルが確立され、かつ適切に運用されているかどうかを確かめることに重点を置いた監査計画となる。例えば、IT 投資管理や情報セキュリティ対策が、PDCA サイクルに基づいて、組織体全体として適切に管理されているかどうかに関する監査計画が必要となる。なお、継続的モニタリングの実施により、PDCA サイクルのどこかに機能の不十分な点や重大なリスクが識別された場合には、それらの点につい

て監査を優先的に行うために監査計画を変更することも必要である。

③ コントロールの視点:IT システムの利活用に係るコントロールを監査対象とする場合、業務プロセス等において、リスクに応じたコントロールが適切に組み込まれ、機能しているかどうかを確かめることに重点を置いた監査計画となる。例えば、規程に従った承認手続が実施されているかどうか、異常なアクセスを検出した際に適時に対処及び報告がなされているかどうか等に関する具体的な監査計画が必要となる。なお、ここでいうコントロールには、手作業によるコントロールと、情報システムに組み込まれた自動化されたコントロールの双方が含まれることに留意する。

コントロールが適切に実施されることによって、情報システムの有効性、効率性、信頼性、安全性（機密性、完全性、可用性)、準拠性が維持される。

④ 統合的視点：上記①～③の視点に加えて、必要な場合は、組織体の目的に達成を効果的かつ効率的に支援する IT システムの目的が達成されるようにガバナンス、マネジメント、コントロールが体系的に統合されて有効に機能しているかも監査の視点に含めなければならない。

2. リスク・アプローチ

(1) システム監査におけるリスク・アプローチとは、IT システムに係るリスクの大きさに応じて監査の人員や時間を充てることにより、監査を効果的かつ効率的に行う監査の実施方法である。リスクの大きさは、脅威と脆弱性が決定要因となるリスク発生可能性とリスクが発生した場合に組織体が受ける影響度の組合せで評価される。

重大なリスクが存在する領域に対して漏れなく監査を行い、かつその領域に存在する重要な脅威や脆弱性（統制の不備)、リスクを適切に発見する監査を効果的・効率的を行うためにリスク・アプローチで監査計画(監査スケジュール(時期と期間)、監査資源、予算、監査の方法等）を作成する。

(2)　リスク・アプローチの監査を実施する前提となるのは、監査対象に対する適切なリスクの識別、分析、評価と、監査実施に係る適切なリスクの識別、分析、評価である。

システム監査において、監査対象に対するリスクとは、組織体の目的達成や戦略遂行において、IT システムの利活用が果たすべき目標（あるべき姿）と実際（現状）との間で差異が発生する可能性とその影響の大きさである。

システム監査に係るリスクには、監査対象に対するリスクと監査実施に係るリスクがある。

監査対象に対するリスクは、固有リスク、統制リスク、残存リスクに分けられる。

① 固有リスク：関連するコントロールが存在しないとの仮定の上で、IT システムに係るリスクで、経営戦略と IT 戦略との不整合、業務プロセス上における情報システムの機能不全、情報漏洩等により、情報システムの有効性、効率性、信頼性、安全性、コンプライアンスが維持されないリスクをいう。

② 統制リスク：IT システムの利活用に係るコントロールの不備・不足により、固有リスクの顕在化等の望ましくない状況や状態に対して、発生防止や適時の発見、是正がなされないリスク。

③ 残存リスク：固有リスクに対してコントロールが施された後も残っているリスク。

また、監査実施に係るリスクとは、組織体に対して重要な影響を与えるリスクを発見できない等、監査の目的が達成できない可能性を合理的に低い水準にまで抑えられないリスクをいう。

監査計画策定においては、まず監査対象全般についてのリスクの識別、分析、評価が行われ、そのリスク評価に基づいて、監査範囲の絞り込みや、監査時間、監査資源、予算、監査の方法等を含んだ監査計画を策定することになる。したがって、リスク・アプローチとは、監査の網羅性（監査対象全般に対するリスク評価）と効率

性（リスクに応じた監査の実施）を両立させるための方法である。

なお、保証を目的としたシステム監査計画策定における監査対象先の選定や監査の優先度は、主として残存リスクの評価に基づき決定されるが、固有リスクや統制リスクについても同時に考慮される必要がある。また、固有リスクと統制リスクは結合して評価する方が望ましい場合が多く、両者を区別して評価することにこだわるとリスク評価が形式的になるおそれがある。

一方、助言を目的としたシステム監査は、システム監査の依頼者と監査人との合意により監査の内容が決定される。その場合、監査の内容についての協議は、統制リスク評価に基づいてなされる場合もあれば、残存リスク評価に基づいてなされる場合もある。

(3) ITガバナンスに係るリスクは、ITガバナンス機能がITシステムの利活用に係る、法的要求事項を満たしていないリスクと経営判断を誤るリスク、監督が不十分なリスク、さらにはITシステムの利活用が組織体の求める目標（経営計画や経営戦略の達成のためのITシステムの利活用に係る目標）を十分に達成していないパフォーマンスに係るリスクに分けることができる。これらのリスクが顕在化することのないように、取締役会等は、適切で十分な情報に基づき判断を行い（判断過程）、かつその判断が著しく不合理でないこと（判断内容）が求められる。判断過程の適切性と判断内容の合理性を確保するために、各取締役は相互監視しかつ取締役会等として監督機能を果たすことになり、これらがガバナンスに係るコントロールの役割を果たすこととなる。監査役（会）等は、ガバナンスにおける監査機能として、取締役会の機能発揮状況、取締役の職務の執行を監査する。ガバナンスの良し悪しの結果がマネジメント、コントロールにおいて具体的事象として出現するので、上記(2)のリスク評価の結果は、ガバナンスに係る監査計画策定の際にも有用である。

(4) 監査計画の見直しについては、組織体内外の環境の変化によりリスクが相当程度変化した場合に検討し、必要な場合は適時適切に監

査計画を変更すべきである。

3. その他

(1) 監査計画の策定に当たっては、リスク評価とともに、必要に応じてリスク評価以外の諸点も考慮する必要がある。

(2) IT システムの利活用に係る助言業務を依頼された場合には、助言業務提供による組織体への貢献度、保証型監査実施への影響、上限提供能力等について検討する必要がある。

(3) 監査計画を策定する際には、効果的・効率的にシステム監査を行うために必要な監査資源が識別される必要があり、適切かつ十分な監査資源は、システム監査を行う組織の長の責任により確保されなければならない。監査資源管理には他の監査やモニタリングの機能との連携、IT ツールの活用、専門家やアウトソースの活用も含まれる。

また、監査のテーマや目的によっては、システム監査以外の監査を担当する業務監査とシステム監査が一体となって監査を行う統合監査の実施も検討される必要がある。

(4) システム監査を外部に委託する場合には、外部委託する組織の長の承認を得る必要がある。

【基準７】監査計画の種類

監査計画は、原則として中長期計画、年度計画、及び個別監査計画に分けて策定されなければならない。

＜主　　旨＞

システム監査を効果的かつ効率的に行うためには、監査計画を、中長期的な対応が必要な事項（中長期計画）と、リスク・アプローチに基づき年間において監査を実施すべき事項（年度計画）と、年間監査計画に基づいて実施する個々の監査のための計画（個別監査計画）に分けて、策定するのが有益である。

＜解釈指針＞

1. 監査計画は、中長期計画、年度計画、及び個別監査計画に分けて策定される。
2. 中長期計画とは、システム監査の中長期における方針等を明らかにすることを目的として作成する。システム監査を経営に貢献するものとするために、又は利害関係者に対する説明責任を果たすために、情報システムの中長期計画と整合を取り、システム開発・更改計画やIT基盤の構築・更改等を踏まえて、システム監査の中長期計画を策定する。
3. 年度計画とは、中長期計画に基づいて、システム監査の年間スケジュールを内容とするものをいう。基本計画とも呼ばれる。
4. 個別監査計画とは、年度の基本計画に基づいて、個々のシステム監査対象ごとに、具体的な監査スケジュールまで落とし込んだ詳細計画書をいう。
5. 原則として、長期計画、年度計画、及び個別監査計画は全て、リスク・アプローチにより策定される必要がある。

【基準８】監査証拠の入手と評価

適切かつ慎重に監査手続を実施し、監査の結論を裏付けるための監査証拠を入手しなければならない。

＜主　　旨＞

監査手続の実施結果として監査証拠が入手され、監査証拠に基づいて監査の結論が形成される。監査手続に基づく監査証拠の入手は、監査の結論を得るために必要不可欠なものである。

＜解釈指針＞

1. 個別監査計画に基づいて、監査手続を実施することによって、監査証拠を入手する。
2. 監査手続は、予備調査（事前調査ともいう。）と本調査に分けて実施する。
   (1) 予備調査とは、監査対象の実態(例えば、情報システムや業務等の詳細、事務手続・マニュアル等による業務内容や業務分掌、組織図等による体制など）を把握するプロセスをいう。
   (2) 予備調査で必要な情報を入手する方法には、例えば、関連する文書や資料等の閲覧、監査対象先のみならず、関連部門へのインタビュー等がある。
   (3) 本調査とは、監査の結論を裏付けるために、十分かつ適切な監査証拠を入手するプロセスをいう。十分かつ適切な監査証拠とは、証拠としての量的十分性と、確かめるべき事項に適合しかつ証明力を備えた証拠をいう。
   (4) 証拠としての十分性及び適切性を確保するためには、単にインタビュー等による口頭証拠だけに依存するのではなく、それを裏付ける書類等の書面による証拠を入手したり、現物等と照合、実際の操作状況を観察したりさらにはテストの実施、詳細な分析等を実施する必要がある。
3. 監査手続の適用に際しては、チェックリスト法、ドキュメントレビュー法 インタビュー法、ウォークスルー法、突合・照合法、現地調査法、コン

ピータ支援監査技法等が利用できる。

4. 監査手続は、それぞれ単独で構成される場合もあるが、一般的には、一つの監査目的に対して複数の監査手続の組合せによって構成される。

5. アジャイル手法を用いたシステム開発プロジェクト等、ドキュメントの作成に重きが置かれない開発手法が採用されている場合には、ウォータフォール等の従来型開発手法とは作成されるドキュメントの種類やドキュメントの作成タイミングが異なることを十分理解し、開発手法に応じた監査証拠を入手することにより、開発現場への負荷増とならないように考慮することが望ましい。

6. また、必要となる監査証拠を適時に入手するために開発の関係者間の意思疎通を図る情報共有、コミュニケーションの仕組み、ルールが整備され、適切にルールが運用されているかを確かめることが重要である。

【基準９】監査調書の作成と保管

監査の結論に至った過程を明らかにし、監査の結論を支える合理的な根拠とするために、監査調書を作成し、適切に保管しなければならない。

＜主　　旨＞

監査調書とは、実施した監査手続、入手した監査証跡及び監査人が到達した結論の記録をいい、かつ、監査の結論の基礎となるものであることから、秩序ある形式で作成し、適切に保管しておく必要がある。

＜解釈指針＞

1. 監査実施内容の適切性・再現性等を確保するために、監査調書を作成する。
2. 監査調書の記載事項には、一般的に、以下の事項が含まれる。ただし、これらに限定されない。
   - 監査実施者及び実施日時
   - 監査の目的
   - 監査手続
   - 監査証拠（監査結果を立証するための資料、データ、証言、監査証跡を含む記録等の全て）
   - 監査手続に基づき確かめた結果
   - 発見事実（事態・事象、真因、影響等）及び発見事実に対する所見
   - 監査調書のレビューが行われた場合には、レビューアの氏名及びレビュー実施日
3. 監査調書に記載されたシステム監査人の所見は、監査結果の結論をまとめるための合理的根拠となる。
4. 別途定められた手続に従って監査調書を体系的に整理し、後日、容易に参照、活用できるように保管する必要がある。
5. 監査調書には、組織体の重要情報や機密情報が記載されていることから、受渡や持出等のルールを定めるとともに、未承認アクセスに対する防止対策、及びバックアップ対策を講じる。

【基準１０】監査の結論の形成

監査報告に先立って、監査調書の内容を詳細に検討し、合理的な根拠に基づき、監査の結論を導かなければならない。

＜主　　旨＞

監査報告に先立って、監査調書に基づいて監査の結論を導く必要がある。保証目的、助言目的に関わらず合理的な根拠に基づき監査の結論を導かなければならない。

＜解釈指針＞

1. 監査の結論を導くための合理的な根拠を得るまで監査手続を実施することで、十分かつ適切な監査証拠を入手する必要がある。
2. 監査調書に基づいて、論理の飛躍がないようにする必要がある。
3. 監査の結果、IT システムのガバナンス、マネジメント、又はコントロールに不備・不足があることが明らかになった場合には、それによる発現可能性のあるリスクの具体的な内容と影響から、残存リスクの大きさを評価し、指摘事項として改善を求めるべきか否かを判断する必要がある。なお、キーコントロールが明らかに不足している場合には、残存リスクの大きさに関わらず原則指摘事項として改善を求める必要がある。監査で発見された不備・不足の全てを指摘事項とする必要はない。また、指摘事項については、残存リスクの大きさに基づき指摘事項の優先順位付けを行う必要がある。
4. 事実確認の結果、指摘事項とすべきと判断した場合には、監査調書に記録された所見、当該事実を裏付ける監査証拠等に基づき、意見交換会や監査講評会を通じて監査対象先に事実認識に相違ないかについて、最終確認を行う必要がある。

［３］システム監査の報告に係る基準

【基準１１】監査報告書の作成と報告

監査報告書は、監査の目的に応じた適切な形式で作成され、監査の依頼者や適切な関係者に報告されなければならない。

＜主　　旨＞

作成された監査報告書は、監査の依頼者である取締役会等及び経営者等や監査対象先等を含む適切な関係者に報告される必要があるが、監査の目的、範囲や結果等の報告すべき内容を理解しやすい方法で報告することが重要である。結果には結論並びに必要な場合改善のための提案及び監査対象先による改善計画、又はそのいずれかを含む。

＜解釈指針＞

1. システム監査報告書の作成に際しては、正確性、客観性、簡潔性、明瞭性、理解容易性、適時性に留意する。また、図（アプリケーションシステムの関係図、処理プロセス図等）、表、グラフ、イラスト、写真等を利用することも効果的である。

   さらに、表現が敵対的になることを避け、建設的なものとすることを心掛ける必要がある。監査報告書の作成に当たっては、監査対象先や関連部門への結果の説明、問題点の相互確認を行う等、事実認識の共有を十分に図る必要がある。

2. システム監査がＩＴガバナンスに関連する場合、取締役会等及び経営者、監査役会等に対する報告と併せて、組織体のガバナンス機能に関わる機関にも監査報告書を提出することが必要である。

3. 監査対象先に対しては、監査報告書の写しを回付する。また、監査対象部門以外にも必要に応じ回付する。

4. 保証を目的とするシステム監査報告書には、監査の目的、範囲及び結果が記載される必要がある。詳細な記載事項やその記載方法は、一様ではないが、以下に例示するような記載を行うことが望ましい。

   (1)　監査の概要

以下に例示する事項を簡潔明瞭に記載する。

- 監査の目的（ニーズ、根拠、背景等でもよい。）
- 監査の対象範囲（その選定根拠等を含むことが望ましい。）
- 監査の実施期間
- 監査の実施者
- （必要に応じて）採用した監査手続の概要

(2) 監査の結果

- 結論
- 指摘事項
- 改善提案及び改善計画（監査報告に際し監査対象先が作成した場合）、又はそのいずれか
- （必要に応じて）総合意見

5. 助言を目的とするシステム監査報告書の様式や記載内容等は、システム監査の依頼者と監査人との間で同意した依頼内容に適したものとする必要がある。

【基準１２】改善提案(及び改善計画)のフォローアップ

監査報告書に改善提案が記載されている場合、適切な措置が、適時に講じられているかどうかを確認するために、改善計画及びその実施状況に関する情報を収集し、改善状況をモニタリングしなければならない。監査報告書に改善計画が記載されている場合も同様にその実施状況をモニタリングしなければならない。

＜主　　旨＞

システム監査は、監査報告書の作成と報告をもって終了するが、監査報告書に改善提案及び監査対象先が作成した改善計画、又はそのいずれかを記載した場合には、当該改善事項が適切かつ適時に実施されているかどうかを確かめておく必要がある。なお、監査人は、改善の実施そのものに責任を負うことはなく、改善の実施が適切であるかどうかをフォローアップし、取締役会等及び経営者等に報告することになる点に留意する。

＜解釈指針＞

1. 監査人は、監査報告書に記載した改善提案への対応状況について監査対象先又は改善責任部門等から、一定期間以内に、具体的な改善内容と方法、実施体制と責任者、進捗状況又は今後のスケジュール等を記載した改善計画書を受領し、適宜、改善実施状況報告書等によって改善状況をモニタリングする必要がある。監査報告書に監査対象先の作成した改善計画を記載する場合も、同様に改善状況をモニタリングする。
2. フォローアップは、監査対象先の責任において実施される改善を監査人が事後的に確認するという性質のものであり、監査人による改善計画の策定及びその実行への関与は、独立性と客観性を損なうことに留意すべきである。
3. 監査対象先から提出された改善実施状況報告書により、改善内容の妥当性、改善体制、改善の進捗状況等を確認し、監査人の改善提案の基となった指摘事項の重大性等を総合的に勘案して、追加的な検証が必要かどうか、あるいは次回以降の監査に反映すべき点がないかどうかを検討

することが望ましい。

4. 監査対象先又は改善責任部門が実施した改善策が不十分であるか、又は改善提案に基づく問題解決がなされないまま放置されている場合は、当該部門に対して、再度の改善対応を要請する必要がある。また、改善が適切かつ適時に行われない場合のリスクを明確にして、取締役会等及び経営者等に報告することが必要な場合もある。

5. フォローアップの終了後、フォローアップ報告書を作成し、監査対象先又は改善責任部門に回付する必要がある。また、重要度に応じ経営者、取締役会等にも報告する。

システム監査基準・システム管理基準の共通用語集（分類別）

分類	用語	定義
ガバナンスとマネジメント関係	ガバナンス	ガバナンスは、次のことによって組織体の目標の達成を保証することである。ステークホルダーを特定し、協議し、そのニーズを明確にして対応する（ステークホルダーへの対応：Engage Stakeholders）、現在と将来のあるべき姿を比較分析し、期待する効果と必要な資源、想定されるリスク等を評価し、判断すること（評価：Evaluate)、IT 戦略と方針を実現するために必要な責任と資源等を組織体内へ割り当て、期待する効果(IT パフォーマンスの期待値を含む)を示し、その実現と想定されるリスクへの対処を経営者に指示すること(指示：Direct)こと、及び戦略で設定した目標をどの程度満たしているか、方針を遵守しているか、パフォーマンスをどの程度達成しているか、また想定したリスクの発現状況及び対処状況について、適切な仕組みを通じて、パフォーマンスの情報を収集し、確認すること(モニタ：Monitor)ことである。ガバナンスは、リスク・マネジメントやコントロールの基となる機能である。ほとんどの組織体において、取締役会等の統治機関がガバナンス全体の責任を負う。統治機関には、上記の活動の実行責任と、適切に遂行していることを示す説明責任の両方を果すことが求められる。
	マネジメント	ガバナンスによって設定された方向に、組織体の目標を達成させるために、戦略やリスク管理

		を計画(Plan)し、体制等を構築(Build)し、業務を運営(Run)し、そしてその運営状況や目標達成状況等をモニタリング(Monitor)する活動である（PBRM)。
	リスク・マネジメント	ガバナンスから示された組織体の目的・目標達成に関し、合理的な保証を提供するために、発生する可能性のある事象や状況（機会、リスク）を識別、評価し、コントロールするプロセス。
	コントロール	リスク・マネジメントのために取られる全ての管理手段。組織的、人的、技術的、物理的な手段がある。統制ともいわれる。
IT ガバナンスと IT マネジメント関係	IT	IT（情報技術）とは、元来はコンピュータを使用して、あらゆる種類の電磁的データや情報を収集、処理、加工、保存、発信、変換する技術のことである。ただし、本基準では、デジタル技術やセンサー等による情報収集技術等、より幅広いテクノロジーも含めて、IT の用語を用いている。
	情報システム	情報システムとは、IT を駆使して業務の流れ(ビジネス・プロセス）の有効性、効率性を高めるための仕組みや、ハードウエア、ソフトウェア、ネットワーク等を指す。
	データ・情報	本基準では、一般的な情報（information)、情報システムに入力された情報であるデータ、そのデータの分析や加工等から見出された組織体やその構成員にとって意味のある情報（intelligence）を指す。
	IT システム	IT、情報システム、データ・情報をまとめた概念を指す。

	IT システムの利活用	IT と情報システムの利活用、情報・データの利活用をまとめた概念であり、組織体の目的や目標の達成のために、IT システムを用いることをいう。IT システムの利活用には、IT システムの利活用を企画、計画するプロセスと、その企画、計画に基づいて、電磁的データや情報を収集、処理、加工、保存、発信、変換するために IT システムを用いるプロセスがある。したがって、組織体内部における IT の計画、調達、外部委託、設計、統合、検証、移行、運用、保守及び廃棄のプロセスの他、外部 IT サービスの調達及び利活用のプロセスが含まれる。
	IT ガバナンス	IT ガバナンスとは、組織体のガバナンスの構成要素で、取締役会等がステークホルダーのニーズに基づいて、組織体の価値及び組織体への信頼を向上させるための IT システムの利活用に係る機能である。具体的な機能は、組織体における IT システムの利活用のあるべき姿を示す IT 戦略と方針の策定、経営者へのその実施指示、及び経営者への実施状況に係る監視、監督である。ほとんどの組織体において、取締役会等の統治機関がガバナンス全体の責任を負う。統治機関には、上記の実行責任と、適切に遂行していることを示す説明責任の両方を果すことが求められる。
	IT マネジメント	経営方針及び IT ガバナンス方針に基づいて策定した IT 戦略の各目標を達成するために、具体策を計画(Plan)し、体制等を構築(Build)し、業務を運営(Run)し、そしてその運営状況や目標達成

		状況等をモニタリング(Monitor)する活動である（PBRM)。
	IT システムに係るリスク	IT システムに係るリスクとは、IT システム自体に対するリスクだけでなく、IT システムに係る戦略や投資、使用する技術、IT システムを用いるビジネス・プロセス、IT システムを管理し使用する組織や人員、そのための方針や規程類、情報システムを配置し、格納する設備や施設、取り扱う情報やデータ等のITシステムに関連するあらゆるリスクを意味している。その観点から、ITシステムに係るリスクと、「係る」という用語を用いている。
組織関係	組織体	一定の共通目標を持つ人々の集合体。会社のような営利活動を行うための経済的組織体と、非営利法人や行政組織のような非経済的組織体とがある。
	ステークホルダー	狭義には株主、投資家、顧客、従業員、取引先、地域社会、行政機関等を指すが、広義には組織体に影響を及ぼす法令や指針等、社会的責任等、広く組織を取り巻くものが含まれる。
	取締役会等	会社の取締役会、非営利法人の理事会等の監督機関を指す。
	監査役（会）等	指名委員会等設置会社の監査委員会及び監査委員、監査等委員会設置会社の監査等委員会及び監査等委員、監査役設置会社の監査役会及び監査役、並びに非営利法人の監事会及び監事、等を指す。
	経営者	業務執行に責任を有する 1 名以上の者を指し、最高経営者だけでなく、業務執行を担う取締役、

		執行役、執行役員等も含む。役割に応じて、CEO、COO、CIO、CISO 等と呼ばれることもある。
	業務分掌	会社等の組織体において、各々の部署やチーム等の業務の目的、範囲、内容、権限、責任を明確化したものをいう。

システム監査基準の用語集（五十音順）

用語	説明
CAAT （コンピュータ支援監査技法）	大量のデータの検索、抽出、計算等を、監査支援専用ソフトウェア等の自動化された監査ツールを使って行い、監査の一部又は全部を効果的・効率的に実施する技法を指す。
外観的独立性	監査対象先から独立した立場で実施されているという外観が確保されており、第三者からみて監査人の精神的独立性が堅持されていないと判断される状況にはないことをいう（「独立性」を参照のこと）。
監査計画	監査計画は、効果的・効率的な監査を実施するために、監査の基本方針を策定し、監査の具体的内容（例えば、目的・目標、実施時期、適用範囲、及び監査の方法等）を決定したものを指す。原則として、中長期計画、年度計画、個別監査計画に大別される。
監査講評会	当該監査を担当した監査人及び監査対象部署等の責任者をはじめとする関係者が集まり、監査の結果に基づく事実関係や発見事項を確認し、指摘事項・改善提案について共通の認識を持つためのミーティングを指す。
監査対象先	監査人が実施する監査の対象となる組織体、部門、部署、業務、機能、プロセス、個別の情報システム、等の監査対象を指す。
監査人	システム監査を行う者を指し、専門職としてのシステム監査人だけでなく、何らかの形でシステム監査を行う人やチーム、集団等を指

	す。
監査の依頼者	内部監査部門や外部監査提供者に監査を依頼する者を指し、助言を目的とした監査においては、取締役会や社長等の経営者、及び業務執行部門等が監査の依頼者となる。また、外部監査においては、保証を目的とした監査においても、組織体外部の第三者に監査の実施を依頼する監査の依頼人が存在し、取締役会や社長等の経営者等が依頼人となる。
監査の利用者	監査結果を利用する者を指し、保証を目的とした監査においては、取締役会や社長等の経営者等が監査の利用者となる。また、監査役（会）等の監査においては、株主が第一次の利用者になる。
監査の結論	監査員が発見した客観的証拠を基に、監査目的及び業務の運用状況を加味した上で下す監査の結果を指す。
監査報告書	監査結果を適切な関係者に伝えるための文書を指す。その形態や形式等は様々で、取締役会や経営者へは監査報告書を提出し、その他の関係者へは監査報告書の写しを回付する場合や、監査対象部門等へ交付する文書を監査結果通知と呼ぶ場合もある。
客観性	監査業務において、バイアス（先入観等）、利益相反を排し、個人や組織等から不当な影響を受けることなく、監査人としての判断を行うことをいう。
契約書等の文書	契約内容を記した文書を指し、契約書だけでなく、覚書等も含む。

再現性	他の標準的な監査人が監査を実施した場合であっても同じ検証結果を得られることをいう。
システム監査を行う組織	システム監査を行う監査人が所属する組織（部門、部署等）を指す。
システム監査を行う組織の長	システム監査を行う組織のマネジメントを行う職責を負う者を指す。
所見	監査で発見したこと、又は発見したことに基づく考えや意見を指す。
助言を目的としたシステム監査	助言及びそれに関連した依頼者向けの業務活動。その活動の目的、内容と範囲は、依頼者と監査人との合意によるものであり、監査人が経営者や管理者としての職責を負うことなく、組織体に価値を付加し、組織体の IT システムに係るガバナンス、リスク・マネジメント、及びコントロールの各プロセスを改善することを意図した活動を指す。
精神的独立性	誠実に行動し、客観性を保持という精神的な態度を堅持できることをいう（「独立性」を参照のこと）。
正当な懐疑心	何事をも当然のこととせず、疑ってみる、又は確認してみる心をいう。
正当な注意	監査の実施過程で監査人として当然払うべき注意をいう。
専門家	特定の分野における専門的な知識、技能、経験を有する者又は組織体を指す。経済産業省のシステム監査制度においてシステム監査企業台帳に登録された企業、公認会計士、監査法人、公認内部監査人（CIA）、公認システ

	ム監査人、公認情報システム監査人（CISA）、コンサルタント等が含まれる。
適切な関係者	監査結果を活用し得る立場にある組織、監査対象先はもとより、監査役やガバナンスに関連する部署等も含まれる。
独立した第三者	組織体の外部にあり、組織体とシステム監査に関する利害を共にしない者又は組織を指す。
独立性	独立性は、第三者から不当な影響や圧力等を受けていない状態を指し、精神的独立性と外観的独立性から構成される。
ニーズ	システム監査の利用者（保証を目的とした監査業務の場合）又は依頼者（助言を目的とした監査業務の場合）による、システム監査に対する要求するあるいは期待する事項、事柄を指す。
文書化された規程等	組織体内部の規程類や、外部委託に際しての契約書等の文書等を指す。
保証を目的としたシステム監査	組織体の IT システムに係るガバナンス、リスク・マネジメント、及びコントロールの各プロセスについての独立的評価を提供する目的で、証拠を客観的に検証・評価する活動を指す。
リスク・アプローチ	監査実施の優先度（監査対象の選定、監査時間や監査資源の配分等）を監査対象先のリスクの大きさに基づいて決定する監査実施の方法を指す。リスク・ベース監査、等ともいわれる。